PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 9/08, 9/30

A1

(11) International Publication Number: WO 00/05836

(43) International Publication Date: 3 February 2000 (03.02.00)

(21) International Application Number: PCT/IL99/00361

(22) International Filing Date: 5 July 1999 (05.07.99)

(30) Priority Data:
125222 6 July 1998 (06.07.98) IL

(71) Applicant (*for all designated States except US*): CIPHERIT LTD. [IL/IL]; Sigalon Street 38, 84965 Omer (IL).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): ARAZI, Benjamin [IL/IL]; Sigalon Street 38, 84965 Omer (IL).

(74) Agents: LUZZATTO, Kfir et al.; Luzzatto & Luzzatto, P.O. Box 5352, 84152 Beer-Sheva (IL).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: A KEY-AGREEMENT SYSTEM AND METHOD

(57) Abstract

A method for carrying out a key distribution process, whereby each member (Useri) who uses the services of a Certifying Authority (CA) is provided with a member's public key (PUi) and a member's private key (si), wherein said process is effected over a finite group of points comprising the steps of: (1) permitting said Certifying Authority to select a generating group-point (G); (2) to generate a random Certifying Authority private key (d); (3) to generate a Certifying Authority public key (PS) (PS=d*G); (4) permitting said member (Useri) to generate a first member's random value (xi) and calculate a first intermediate member's public key (xi*G); (6) permitting said Certifying Authority to calculate said member's public key (PUi) and member's intermediate private key (pi), wherein: a second member's random value (yi) is generated and a second intermediate member's public key (yi*G) is calculated, said member's public key (PUi) is calculated: PUi = xi*G + yi*G, a member's temporary value (H(IDi, PUi)) is calculated by operating with a hash transformation (H), said member's intermediate private key (pi) is calculated (pi=H(IDi, PUi)*d+yi); (7) permitting said member to generate said member's private key (si) (si=pi+xi).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

A KEY-AGREEMENT SYSTEM AND METHOD

Field of The Invention

The present invention relates to systems and methods for efficiently generating a secret key joint to two communicating parties, based on any exponentiation method in the broad sense of the word, including keys generated by operations over elliptic curves and keys generated by modular exponentiations over finite fields or groups.

Background of the Invention

A 'key agreement system' refers to the case in which two users exchange public (non-secret) values, over an unprotected communication channel, for the purpose of ending up with a joint key, termed 'session key', where both users have a session key of the same value, without any other party who listens to the exchanged information being able to generate the same session key.

The generation of joint session keys is important in a variety of applications, particularly for protecting information transmitted over communication channels.

A fundamental key agreement system was proposed in [W. Diffie and M. E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, IT-22, pp. 644-654, 1976]. This system, hereinafter referred to as the DH key agreement system and which is well known to persons skilled in the art, concerns two parties which generate a session key by operating over an agreed finite field GF(p) and using an agreed element g of said field. Party P1 and P2 respectively have private keys x and y and public keys $g^x \bmod p$ and $g^y \bmod p$. A secret key K joint to said parties is then generated by exchanging said public keys. Said party P1 generates said K by applying a generation method which involves calculating $(g^y \bmod p)^x \bmod p$. Said party P2 generates the same said K by calculating $(g^x \bmod p)^y \bmod p$. For a large prime p it is assumed that said key K can be known only to said two parties.

In said DH key agreement system two specific parties always generate the same session key whenever they wish to generate such a key, while no authentication is provided. That is, a communicating party is not assured of the identity of his counterpart. Authenticity proof in provided by the existence of a CA (Certifying Authority) that issues a signature which witnesses the association between a user's public key and said user's identification details. Said signature is termed 'certificate' and is owned and submitted by said user whenever he submits his public key.

A signature generation and verification technique relevant to this system can be based on recognized methods, such as the DSS [National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Register, pp. 42919-43546, August 30, 1991].

In a system hereinafter referred to as "ephemeral-key-agreement system", two users generate a different session key whenever they wish to generate such a key, based on a random value generated by each user, while they are mutually authenticated in the sense that each communicating user is assured that a public key submitted by a party which purports to be Useri was truly submitted by a party that proved to said CA at some preliminary stage that it possesses Useri's identification details.

An ephemeral-key-agreement system can be based on said extended DH key agreement system where party P1 and P2 respectively generate random values x and y and non-secret values g^x mod p and g^y mod p where each of said parties signs his said non-secret value using a digital signature procedure. The public key of each party, which is also sent to the other party together with a certificate, is the public key needed for verifying that party's signature.

DSS verification procedure involves two exponentiation operations. This means that the above ephemeral-key-agreement system involves the following exponentiation operations:

1. Generation of an ephemeral value;
2. Generation of a signature on said ephemeral value;

(The above two values are sent to the other party)

3-4. Two exponentiations involved in DSS verification of the certificate;

5-6. Two exponentiations involved in DSS verification of said signature on the ephemeral value.

(Operations 3-6 are performed on data received from the other party.)

An ephemeral-key-agreement system can further be based on the MQV system [L. Law, A. Menezes, M. Qu, J. Solinas and S. Vanstone, "An Efficient Protocol for Authenticated Key Agreement", Technical Report CORR 98-05, Dept. of C&O, University of Waterloo, Canada, March 1998]. Like with the said DH key agreement system the MQV system also requires that the public key of each party be sent to the other party together with a certificate. If the signature generation and verification operations relevant to this system are based on the said DSS, a MQV-based ephemeral-key-agreement system involves the following exponentiation operations:

1. Generation of an ephemeral value;

2-3. Two exponentiations involved in DSS verification of the certificate;

4-5. Two exponentiations involved in the generation of the ephemeral key.

Given an integer g and a value g^r mod p for a given p, where the exponent r is unknown, the general problem of recovering r is defined in the art as a discrete logarithm problem, whose solution (that is, the recovery of r) is considered to be highly complex for a large prime p. Given a point G and a point $Q = r*G$ on an elliptic curve whose equation is known, where the scalar r is unknown, the general problem of recovering r is also considered in the art as a discrete log problem. Furthermore, the operation of multiplying a point on an elliptic curve by a scalar is also termed in the art as an exponentiation operation (in which the point is the base and the scalar is the exponent).

DH key agreement and MQV systems can also be implemented over elliptic curves, as indicated in [IEEE P1363 Working Draft, February 1998.]

Values like g^x mod p, or points like xG on an elliptic curve, are generally termed 'group-points of a finite group in which the discrete log problem applies'.

The large number of exponentiation operations performed in the execution of said DH system and said MQV system (6 operations in a DH system and 5 in an MQV system) stems from a need to explicitly certify user's public keys, resulting an explicit certificate verification which requires two exponentiations.

Thus, the art has so far failed to provide means by which key-agreements can be effectively implemented by saving exponentiations associated with the explicit certificate verification of user's public keys.

SUMMARY OF THE INVENTION

In one aspect the invention is directed to a method by which each member (Useri) of a plurality of users who use the services of a Certifying Authority (CA) is provided with a member's public key (PUi) and a member's private key (si) for the purpose of effecting a key-agreement process between any two members of said plurality of users, where said process is effected over a finite group of points in which the discrete logarithm problem applies, comprising the steps of:

(1) permitting said Certifying Authority to select a generating group-point (G) whose multiplication by various scalars generate various group-points;

(2) permitting said Certifying Authority to generate a random Certifying Authority private key (d);

(3) permitting said Certifying Authority to generate a Certifying Authority public key (PS) by multiplying said Certifying Authority private key by said generating group-point (PS = d∗G);

(4) permitting said member (Useri) to generate a first member's random value (xi) and calculate a first intermediate member's public key (xi∗G) by

multiplying said first member's random value by said generating group-point;

(5) permitting said member (Useri) to submit said first intermediate member's public key (xi∗G) and the member's identification details (IDi) of said member to said Certifying Authority;

(6) permitting said Certifying Authority to calculate said member's public key (PUi) and member's intermediate private key (pi), wherein:

- a second member's random value (yi) is generated and a second intermediate member's public key (yi∗G) is calculated by multiplying said second member's random value by said generating group-point;
- said member's public key (PUi) is calculated by adding said first intermediate member's public key and said second intermediate member's public key (PUi = xi∗G + yi∗G) ;
- a member's temporary value (H(IDi,PUi)) is calculated by operating with a hash transformation (H) which converts a scalar and a group-point into a scalar on said member's identification details (IDi) and said member's public key (PUi);
- said member's intermediate private key (pi) is calculated by multiplying said member's temporary value by said Certifying Authority private key (d) and adding said second member's random value (yi) to the product obtained by said multiplication (pi = H(IDi,PUi)∗d + yi).

(7) permitting said Certifying Authority to submit said member's public key (PUi) and said member's intermediate private key (pi) to said member;

(8) permitting said member to generate said member's private key (si) by adding said first member's random value (xi) to said member's intermediate private key (si = pi + xi).

Another preferred embodiment of the invention relates to an ephemeral-key-agreement system based on the discrete logarithm problem over a finite group of points wherein a first member (Userj) and a second member (Userk) of a plurality of users who use the services of a Certifying Authority (CA), as defined in Claim 1, generate a joint session key, the system comprising:

(1) means for permitting said first member (Userj) to generate a first member's random parameter (rj) and calculates a first member's ephemeral value (EVj) by multiplying said first member's random parameter by the generating group-point (**EVj** = rj∗**G**);

(2) means for permitting said second member (Userk) to generate a second member's random parameter (rk) and calculates a second member's ephemeral value (**EVk**) by multiplying said second member's random parameter by the generating group-point (**EVk** = rk∗**G**);

(3) means for sending the first member's identification details (IDj) and the first member's public key (**PUj**) and said first member's ephemeral value (**EVj**) from said first member to said second member;

(4) means for sending the second member's identification details (IDk) and the second member's public key (**PUk**) and said second member's ephemeral value (**EVk**) from said second member to said first smember;

(5) means for permitting said first member to calculate a first secret key (**Kj**) wherein:

- a first value (sj + rj) is calculated by adding the private key of said first member and said first member's random parameter;

- a second value (H(IDk,PUk)) is calculated by operating with the hash transformation (H) on said second member's identification details (IDk) and said second member's public key (PUk);

- a third value (H(IDk,PUk)*PS) is calculated by multiplying said second value by the public key (PS) of the Certifying Authority;

- a fourth value (H(IDk,PUk)*PS + PUk + EVk) is calculated by adding said third value and said second member's public key and said second member's ephemeral value;

- a fifth value ((sj + rj)*(H(IDk,PUk)*PS + PUk + EVk)) is calculated by multiplying said first value and said fourth value;

- a sixth value (rj*EVk) is calculated by multiplying said first member's random parameter and said second member's ephemeral value;

- said first secret key (Kj) is obtained by adding said fifth and said sixth values (Kj = (sj + rj)*(H(IDk,PUk)*PS + PUk + EVk) + rj*EVk);

- said operations being defined based on the characteristics of said finite group of points.

(6) means for permitting said second member to calculate a second secret key (Kk) wherein:

- a seventh value (sk + rk) is calculated by adding the private key of said second member and said second member's random parameter;

- an eighth value (H(IDj,PUj)) is calculated by operating with the hash transformation (H) on said first member's identification details (IDj) and said first member's public key (PUj);

- a ninth value (H(IDj,PUj)∗PS) is calculated by multiplying said eighth value by said public key (PS) of the Certifying Authority;

- a tenth value (H(IDj,PUj)∗PS + PUj + EVj) is calculated by adding said ninth value and said first member's public key and said first member's ephemeral value;

- an eleventh value ((sk + rk)∗(H(IDj,PUj)∗PS + PUj + EVj)) is calculated by multiplying said seventh value and said tenth value;

- a twelfth value (rk∗EVj) is calculated by multiplying said second member's random parameter and said first member's ephemeral value;

- said second secret key (Kk) is obtained by adding said eleventh and said twelfth values (Kk = (sk + rk)∗(H(IDj,PUj)∗PS + PUj + EVj) + rk∗EVj);

- said operations being defined based on the characteristics of said finite group of points.

(7) means for permitting said first member and said second member to confirm that said first secret key equals said second secret key by encrypting a test message by one of said secret keys and decrypting the result by the other secret key;

whereby said first and second members use said first and second secret keys respectively as the secret key joint to the two of them, and the value of said secret key joint to the two said members is different each time said first and second members generate a joint secret key.

According to a preferred embodiment of the invention users secret keys can be obtained by by operating with a hash transformation on two group-points, converting them into a scalar into a scalar.

According to a preferred embodiment of the invention the multiplication of a group point by a scalar is carried over an elliptic curve.

According to another preferred embodiment of the invention the multiplication of a group point by a scalar is carried by a modular exponentiation over a finite field.

In another aspect, the invention is directed to a method by which each member of a plurality of users who use the services of a Certifying Authority (CA) is provided with a member's public key and a member's private key for the purpose of effecting a key-agreement process between any two members of said plurality of users without said Certifying Authority issuing any explicit certificate which witnesses an association between a member's public key and said member's identification details, where said process is effected over a finite group of points in which the discrete log problem applies, comprising the steps of:

(1) said member's public key is generated by using secret parameters individual to said member where a part of said secret parameters is only known to said Certifying Authority and a part of said secret parameters is only known to said member;

(2) said member's private key is generated by using said Certifying Authority's private key and said member's identification details and said secret parameters individual to said member;

thereby enabling said member to generate a joint secret key with another member of said plurality of users with a mutual authentication and without said Certifying Authority issuing any explicit certificate which witnesses an association between a member's public key and said member's identification details.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

All the above and other characteristics and advantages of the invention, though clear to the skilled person, will be better understood through the following illustrative and non-limitative description of preferred embodiments thereof.

The following notations are used throughout the description of the various embodiments of this invention:

Useri denotes a member of a plurality of users who use the services of a Certifying Authority CA.

IDi denotes the identification details of said Useri.

The term "group-point" refers to an element of a finite group in which the discrete logarithm problem applies.

Group-points are denoted in **bold** letters.

The notation k∗**B** means a multiplication of the group-point **B** by a scalar k. (When operating over GF(q), this notation is replaced by $\mathbf{B}^k$ mod q, for a prime q common to all users. When operating over an elliptic curve, this notation means k**B**, for a point **B** on a curve whose parameters are common to all users.)

G is a generating group point. That is, for any point **B** of the group, except for the 0 point, there is some k such that **B** = k∗**G**.

Scalars are calculated modulo the prime order of the group.

d denotes the private key of the said CA.

PS denotes the public key of the CA, where **PS** = d∗**G**.

si denotes the private key of said Useri.

PUi denotes the public key of said Useri.

H(q,**w**) denotes a hash transformation which converts a scalar q and a group-point **w** into a scalar.

A preferred first embodiment of this invention concerns a method by which a Certifying Authority CA provides personal keys to a general user termed Useri. Said personal keys, which are distinct for each user, are provided for the purpose of effecting key-agreement between two users, while achieving personal identification. That is, each user is assured of the personal identity of his key agreement partner. The calculations are effected over a finite group of points.

The private key of said CA is a scalar d. The public key of said CA is a group-point **PS** where **PS** = d∗**G**, for a generating group-point **G**.

Said Useri generates a random xi and submits xi∗**G** and IDi to said CA, where **G** is said generating group-point and IDi denotes the identification details of said Useri. Said CA generates a random yi, calculates **PUi** = xi∗**G** + yi∗**G** and submits said **PUi** to said Useri, together with pi = H(IDi,PUi)∗d + yi, where H denotes a hash transformation which converts a scalar and a group-point into a scalar.

Said Useri generates his private key si = pi + xi = H(IDi,PUi)∗d + (xi+yi).

The public key of said Useri is said PUi.

A preferred second embodiment of this invention concerns an ephemeral-key-agreement system, wherein Userj and Userk, each being issued personal keys according to said preferred first embodiment of this invention (said index i is general and is replaced by j or k to denote specific users), generate a joint session key.

Said Userj generates a random rj, calculates an ephemeral value EVj = rj∗G and sends to said Userk: IDj, PUj, EVj.

Userk generates a random rk, calculates an ephemeral value **EVk** = rk∗**G** and sends to said Userj: IDk, **PUk**, **EVk**.

Userj calculates **Kj** = (sj + rj)∗(H(IDk,PUk)∗**PS** + **PUk** + **EVk**) + rj∗**EVk**.

Userk calculates **Kk** = (sk + rk)∗(H(IDj,PUj)∗**PS** + **PUj** + **EVj**) + rk∗**EVj**.

Said values **Kj** and **Kk** are the generated session key, joint to said Userj and Userk.

A key confirmation now follows. Here, said users Userj and Userk use the said generated keys **Kj** and **Kk** in order to encrypt and decrypt a selected random value, thereby establishing that they share the same key. That is, they verify that **Kj** = **Kk**.

To prove the validity of the system according to the aforesaid preferred second embodiment of this invention it is noted that

Kj = (sj + rj)∗(H(IDk,PUk)∗**PS** + **PUk** + **EVk**) + rj∗**EVk** =

= (sj + rj)∗(H(IDk,PUk)∗d + xk + yk + rk) + rj∗rk∗**G** = (sj + rj)∗(sk + rk) + rj∗rk∗**G**

which is symmetric in j and k.

The system according to the aforesaid preferred second embodiment of this invention is effected by four exponentiation operations, compared to six exponentiations associated with the DH system and five exponentiations associated with the MQV system.

The expression for the key **Kj** according to said preferred second embodiment of this invention consists of the addend (sj + rj)∗(H(IDk,PUk)∗**PS** + **PUk** + **EVk**) and the addend rj∗**EVk**. Similarly, the expression for the key **Kk** according to said preferred second embodiment of this invention consists of the addend (sk + rk)∗(H(IDj,PUj)∗**PS** + **PUj** + **EVj**) and the addend rk∗**EVj**. Said keys **Kj** and **Kk** can be generated by combining together said two addends, of which each key constitutes, in a way which is not an addition operation. According to a preferred third embodiment of this invention:

$$Kj = H1\big((sj + rj)*(H(IDk,PUk)*PS + PUk + EVk),\ rj*EVk\big)$$

$$Kk = H1\big((sk + rk)*(H(IDj,PUj)*PS + PUj + EVj)\ ,\ rk*EVj\big),$$

where H1 is a hash transformation which hashes the two group-points, separated by a comma, into a scalar.

Notations of the general form k∗B, used hereinbefore, mean a multiplication of the group-point **B** by a scalar k. When operating over the finite field GF(q), this notation is replaced by the modular exponentiation B^k mod q, for a prime q common to all users. When operating over an elliptic curve, this notation means kB, for a point **B** on a curve whose parameters are common to all users. A preferred fourth embodiment of this invention concerns effecting any of the aforesaid preferred first, second and third embodiments of this invention, over a finite field GF(q) and over an elliptic curve.

A preferred fifth embodiment of this invention concerns the method, well clarified in the aforesaid preferred first and second embodiments of this invention, according to which a key-agreement is effected between two users without said CA issuing any explicit certificate which witnesses an association between a user's public key and said user's identification details. It is observed that saving the explicit certification is facilitated by combining two conditions: (1) a user's public key is generated by using secret parameters xi and yi individual to said user, where one parameter (yi) is only known to said CA and one parameter (xi) is only known to said user; (2) said user's private key (si) is generated by using said CA's private key (d) and said user's identification details (IDi) and said secret parameters (xi and yi) individual to said user.

CLAIMS

1. A method for carrying out a key distribution process, whereby each member (Useri) of a plurality of users who use the services of a Certifying Authority (CA) is provided with a member's public key (PUi) and a member's private key (si), wherein said process is effected over a finite group of points in which the discrete logarithm problem applies, comprising the steps of:

   (1) permitting said Certifying Authority to select a generating group-point (G) whose multiplication by various scalars generate various group-points;

   (2) permitting said Certifying Authority to generate a random Certifying Authority private key (d);

   (3) permitting said Certifying Authority to generate a Certifying Authority public key (PS) by multiplying said Certifying Authority private key by said generating group-point ($PS = d*G$);

   (4) permitting said member (Useri) to generate a first member's random value (xi) and calculate a first intermediate member's public key ($xi*G$) by multiplying said first member's random value by said generating group-point;

   (5) permitting said member (Useri) to submit said first intermediate member's public key ($xi*G$) and the member's identification details (IDi) of said member to said Certifying Authority;

   (6) permitting said Certifying Authority to calculate said member's public key (PUi) and member's intermediate private key (pi), wherein:

      - a second member's random value (yi) is generated and a second intermediate member's public key ($yi*G$) is calculated by multiplying said second member's random value by said generating group-point;

- said member's public key (**PUi**) is calculated by adding said first intermediate member's public key and said second intermediate member's public key (**PUi** = xi***G** + yi***G**) ;

- a member's temporary value (H(IDi,**PUi**)) is calculated by operating with a hash transformation (H) which converts a scalar and a group-point into a scalar on said member's identification details (IDi) and said member's public key (**PUi**);

- said member's intermediate private key (pi) is calculated by multiplying said member's temporary value by said Certifying Authority private key (d) and adding said second member's random value (yi) to the product obtained by said multiplication (pi = H(IDi,**PUi**)*d + yi).

(7) permitting said Certifying Authority to submit said member's public key (**PUi**) and said member's intermediate private key (pi) to said member;

(8) permitting said member to generate said member's private key (si) by adding said first member's random value (xi) to said member's intermediate private key (si = pi + xi).

2. A method for carrying out ephemeral-key-agreements based on the discrete logarithm problem over a finite group of points wherein a first member (Userj) and a second member (Userk) of a plurality of users who use the services of a Certifying Authority (CA), as defined in Claim 1, generate a joint session key, the method comprising:

(1) permitting said first member (Userj) to generate a first member's random parameter (rj) and to calculate a first member's ephemeral value (**EVj**)

by multiplying said first member's random parameter by the generating group-point ($EVj = rj*G$);

(2) permitting said second member (Userk) to generate a second member's random parameter (rk) and to calculate a second member's ephemeral value (EVk) by multiplying said second member's random parameter by the generating group-point ($EVk = rk*G$);

(3) sending the first member's identification details (IDj) and the first member's public key (PUj) and said first member's ephemeral value (EVj) from said first member to said second member;

(4) sending the second member's identification details (IDk) and the second member's public key (PUk) and said second member's ephemeral value (EVk) from said second member to said first smember;

(5) permitting said first member to calculate a first secret key (Kj) wherein:

- a first value ($sj + rj$) is calculated by adding the private key of said first member and said first member's random parameter;

- a second value ($H(IDk,PUk)$) is calculated by operating with the hash transformation (H) on said second member's identification details (IDk) and said second member's public key (PUk);

- a third value ($H(IDk,PUk)*PS$) is calculated by multiplying said second value by the public key (PS) of the Certifying Authority;

- a fourth value ($H(IDk,PUk)*PS + PUk + EVk$) is calculated by adding said third value and said second member's public key and said second member's ephemeral value;

- a fifth value ($(sj + rj)*(H(IDk,PUk)*PS + PUk + EVk)$) is calculated by multiplying said first value and said fourth value;

- a sixth value (rj*EVk) is calculated by multiplying said first member's random parameter and said second member's ephemeral value;

- said first secret key (Kj) is obtained by adding said fifth and said sixth values (Kj = (sj + rj)*(H(IDk,PUk)*PS + PUk + EVk) + rj*EVk);

- said operations being defined based on the characteristics of said finite group of points.

(6) permitting said second member to calculate a second secret key (Kk) wherein:

- a seventh value (sk + rk) is calculated by adding the private key of said second member and said second member's random parameter;

- an eighth value (H(IDj,PUj)) is calculated by operating with the hash transformation (H) on said first member's identification details (IDj) and said first member's public key (PUj);

- a ninth value (H(IDj,PUj)*PS) is calculated by multiplying said eighth value by said public key (PS) of the Certifying Authority;

- a tenth value (H(IDj,PUj)*PS + PUj + EVj) is calculated by adding said ninth value and said first member's public key and said first member's ephemeral value;

- an eleventh value ((sk + rk)*(H(IDj,PUj)*PS + PUj + EVj)) is calculated by multiplying said seventh value and said tenth value;

- a twelfth value (rk*EVj) is calculated by multiplying said second member's random parameter and said first member's ephemeral value;

- said second secret key (Kk) is obtained by adding said eleventh and said twelfth values (Kk = (sk + rk)*(H(IDj,PUj)*PS + PUj + EVj) + rk*EVj);

- said operations being defined based on the characteristics of said finite group of points.

(7) permitting said first member and said second member to confirm that said first secret key equals said second secret key by encrypting a test message by one of said secret keys and decrypting the result by the other secret key;

whereby said first and second members use said first and second secret keys respectively as the secret key joint to the two of them, and the value of said secret key joint to the two said members is different each time said first and second members generate a joint secret key.

3. A method according to Claim 2, in which the first secret key is obtained by operating with a hash transformation (H1) on the fifth and sixth values, and the second secret key is obtained by operating with said hash transformation on the eleventh and twelfth values, where said hash transformation converts two group-points into a scalar.

4. An ephemeral-key-agreement system based on the discrete logarithm problem over a finite group of points wherein a first member (Userj) and a second member (Userk) of a plurality of users who use the services of a Certifying Authority (CA), as defined in Claim 1, generate a joint session key, the system comprising:

(1) means for permitting said first member (Userj) to generate a first member's random parameter (rj) and to calculate a first member's ephemeral value (EVj) by multiplying said first member's random parameter by the generating group-point ($EVj = rj*G$);

(2) means for permitting said second member (Userk) to generate a second member's random parameter (rk) and to calculate a second member's ephemeral value (EVk) by multiplying said second member's random parameter by the generating group-point ($EVk = rk*G$);

(3) means for sending the first member's identification details **(IDj)** and the first member's public key **(PUj)** and said first member's ephemeral value **(EVj)** from said first member to said second member;

(4) means for sending the second member's identification details **(IDk)** and the second member's public key **(PUk)** and said second member's ephemeral value **(EVk)** from said second member to said first smember;

(5) means for permitting said first member to calculate a first secret key **(Kj)** wherein:

- a first value (sj + rj) is calculated by adding the private key of said first member and said first member's random parameter;

- a second value (H(IDk,PUk)) is calculated by operating with the hash transformation (H) on said second member's identification details (IDk) and said second member's public key **(PUk)**;

- a third value (H(IDk,PUk)*PS) is calculated by multiplying said second value by the public key **(PS)** of the Certifying Authority;

- a fourth value (H(IDk,PUk)*PS + PUk + EVk) is calculated by adding said third value and said second member's public key and said second member's ephemeral value;

- a fifth value ((sj + rj)*(H(IDk,PUk)*PS + PUk + EVk)) is calculated by multiplying said first value and said fourth value;

- a sixth value (rj*EVk) is calculated by multiplying said first member's random parameter and said second member's ephemeral value;

- said first secret key **(Kj)** is obtained by adding said fifth and said sixth values **(Kj = (sj + rj)*(H(IDk,PUk)*PS + PUk + EVk) + rj*EVk)**;

- said operations being defined based on the characteristics of said finite group of points.

(6) means for permitting said second member to calculate a second secret key (Kk) wherein:

- a seventh value (sk + rk) is calculated by adding the private key of said second member and said second member's random parameter;

- an eighth value (H(IDj,PUj)) is calculated by operating with the hash transformation (H) on said first member's identification details (IDj) and said first member's public key (PUj);

- a ninth value (H(IDj,PUj)*PS) is calculated by multiplying said eighth value by said public key (PS) of the Certifying Authority;

- a tenth value (H(IDj,PUj)*PS + PUj + EVj) is calculated by adding said ninth value and said first member's public key and said first member's ephemeral value;

- an eleventh value ((sk + rk)*(H(IDj,PUj)*PS + PUj + EVj)) is calculated by multiplying said seventh value and said tenth value;

- a twelfth value (rk*EVj) is calculated by multiplying said second member's random parameter and said first member's ephemeral value;

- said second secret key (Kk) is obtained by adding said eleventh and said twelfth values (Kk = (sk + rk)*(H(IDj,PUj)*PS + PUj + EVj) + rk*EVj);

- said operations being defined based on the characteristics of said finite group of points.

(7) means for permitting said first member and said second member to confirm that said first secret key equals said second secret key by

encrypting a test message by one of said secret keys and decrypting the result by the other secret key;

whereby said first and second members use said first and second secret keys respectively as the secret key joint to the two of them, and the value of said secret key joint to the two said members is different each time said first and second members generate a joint secret key.

5. An ephemeral-key-agreement system according to Claim 4 in which the first secret key is obtained by operating with a hash transformation (H1) on the fifth and sixth values, and the second secret key is obtained by operating with said hash transformation on the eleventh and twelfth values, where said hash transformation converts two group-points into a scalar.

6. A method according to Claim 1 in which the multiplications of a point by a scalar are carried over an elliptic curve.

7. A method according to Claim 1 in which the multiplications of a point by a scalar mean modular exponentiations.

8. A key-agreement system according to any one of Claims 2 and 3 in which the multiplications of a point by a scalar are carried over an elliptic curve.

9. A key-agreement system according to Claim 4 or 5, in which the multiplications of a point by a scalar mean modular exponentiations.

10. A method by which each member of a plurality of users who use the services of a Certifying Authority (CA) is provided with a member's public key and a member's private key for the purpose of effecting a key-agreement process between any two members of said plurality of users without said Certifying Authority issuing any explicit certificate which witnesses an association between a member's public key and said member's identification details, where said process is effected over a finite group of points in which the discrete log problem applies, comprising the steps of:

    (1) generating said member's public key by using secret parameters individual to said member where a part of said secret parameters is only known to said Certifying Authority and a part of said secret parameters is only known to said member;

    (2) generating said member's private key by using said Certifying Authority's private key and said member's identification details and said secret parameters individual to said member;

    thereby enabling said member to generate a joint secret key with another member of said plurality of users with a mutual authentication and without said Certifying Authority issuing any explicit certificate which witnesses an association between a member's public key and said member's identification details.

11. A method for effecting key-agreements, essentially as described and illustrated.

12. An ephemeral-key-agreement system, essentially as described and illustrated.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IL 99/00361

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 515 441 A (FAUCHER DAVID W) 7 May 1996 (1996-05-07) abstract column 2, line 5 - line 20 column 4, line 38 -column 5, line 15 column 5, line 54 -column 6, line 3 claim 1 figures 5,9 ---	1-10
A	EP 0 535 863 A (AMERICAN TELEPHONE & TELEGRAPH) 7 April 1993 (1993-04-07) abstract page 3, line 8 - line 16 page 3, line 44 -page 4, line 56 page 5, line 10 - line 13 page 11, line 18 - line 57 claim 1 figures 1,6 ---	1-10

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 October 1999	29/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

1

INTERNATIONAL SEARCH REPORT

In. .ational Application No
PCT/IL 99/00361

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	KENJI KOYAMA ET AL: "ELLIPTIC CURVE CRYPTOSYSTEMS AND THEIR APPLICATIONS" IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS, vol. E75 - D, no. 1, 1 January 1992 (1992-01-01), pages 50-57, XP000301174 ISSN: 0916-8532 the whole document -----	1-9

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IL 99/00361

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5515441 A	07-05-1996	NONE	
EP 0535863 A	07-04-1993	US 5241599 A	31-08-1993
		AU 648433 B	21-04-1994
		AU 2351392 A	08-04-1993
		CA 2076252 A,C	03-04-1993
		JP 2599871 B	16-04-1997
		JP 6169306 A	14-06-1994